ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

March 20, 1997

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, INTELLIGENCE SYSTEMS BOARD
DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: Secret and Below Interoperability (SABI)

References:
(a) Computer Security Act of 1997
(b) NTISSD No. 501, National Training Program for Information Systems Security (INFOSEC) Professionals
(c) NSTISSI No. 4011, National Training Standard for Information Systems Security (INFOSEC) Professionals
(d) NSTISSI No. 4012, National Training Standard for Designated Approving Authority (DAA)
(e) NSTISSI No. 4013, National Training Standard for System Administrators In Information Systems Security (INFOSEC)
(f) NSTISSI No. 4014, National Training Standard for Information Systems Security Officers (ISS0)

This memorandum provides guidance for sharing appropriate information among users and interconnecting systems/networks at secret levels with users and systems/networks down to the unclassified level. Interconnections between Top Secret, including all Sensitive Compartmented Information systems/networks, are not the subject of this memorandum.

Critical operational missions require the movement of appropriate information between Secret and Unclassified systems and have driven many organizations to interconnect such systems. Connecting Secret systems to systems at a lower classification level poses significant security concerns including disclosure of classified information to unclassified users and compromising the

integrity of Secret systems. Application of security configurations with approved security products, uniform risk criterion, trained systems security personnel, and strict configuration control is necessary to mitigating risk.

Since SABI implementations impact directly and indirectly on all organizations interconnected with Secret systems, an infrastructure-centric view is essential. Therefore, effective immediately, the following guidelines are applicable to all organizations with SABI implementations.

a. The Commanders in Chief (CINCs). Service and Agencies will follow a standardized certification and accreditation process, like that described in the draft version of the Department of Defense (DoD) Information Technology Security Certification and Accreditation Process (DITSCAP), when connecting systems. All connected systems will be subject to monitoring in accordance with existing DoD guidelines to ensure that security features are in place and working.

b. The National Security Agency (NSA) will publish and periodically update a listing of available SABI security implementations, concepts of operation, and products. The CINCs, Services and Agencies will adhere to these when connecting Secret systems/networks down to Unclassified systems/networks. All implementations must satisfy connection criteria of the cognizant connection approving authority. Products shall be configured in accordance with their associated concepts of operation to satisfy connection criteria. Organizations currently using non-approved Secret and below security implementations will bring their systems into compliance by the end of fiscal year 1998.

c. NSA, working with the Defense Information Systems Agency (DISA), will provide system security engineering services to assist the CINCs, Service and Agencies in finalizing site-specific SABI implementations.

d. Services and Agencies using SABI implementation will expand existing training curricula to include Information System Security (INFOSEC) training of personnel appointed as Designated Approving Authority (DAA), Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO), and system administrators in accordance with references (a), (b), (c), (d), (e), and (f). Personnel who use, operate, or maintain Secret and below systems require appropriate security training. DISA will develop generic INFOSEC training material for use in the CINCs', Services' and Agencies' programs.

e. NSA will take the lead with DISA, Joint Staff, CINCs, Services, and Agencies to establish a process and common acceptable minimum risk level for networks affected by SABI implementations. This will be accomplished within six months and will be reassessed every six months.

f. Together NSA and DISA will take the lead in coordinating a community effort to develop and execute a joint vulnerability assessment process, including evaluation and development of automated tools for measuring system risks that will operate against SABI implementations to ensure defense information infrastructure (DII) sustained integrity. A quarterly report documenting the results of the assessment, along with system security recommendations, will be provided to the cognizant DAA.

My point of contact for this action is Mr. Morris Hymes, Jr., who is assigned to the Office of my Deputy Assistant Secretary of Defense for Command, Control and Communications, telephone (703) 637-5936, E-mail morris.hymes@osd.pentagon.mil.

Emmett Paige, Jr.